

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
KEEP Tookit	SQL injection vulnerability in lib/patUser.php in KEEP Toolkit before 2.5.1 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password.	2009-01-27	7.5	CVE-2009-0287 BID CONFIRM
activewebsoftwares -- active_business_directory	SQL injection vulnerability in default.asp in Active Business Directory 2 allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2009-01-26	7.5	CVE-2008-5972 BID MILWORM FRSIRT SECUNIA
activewebsoftwares -- active_web_mail	SQL injection vulnerability in login.aspx in Active Web Mail 4.0 allows remote attackers to execute arbitrary SQL commands via the password parameter.	2009-01-26	7.5	CVE-2008-5973 XF MILWORM SECUNIA
	Multiple SQL injection vulnerabilities in login.aspx in Active			CVE-2008-5874

activewebs softwares -- active_price_comparison	Price Comparison 4.0 allow remote attackers to execute arbitrary SQL commands via the (1) password and (2) username fields.	2009-01-26	7.5	2274 MILWORM FRSIRT SECUNIA
activewebs softwares -- active_price_comparison	SQL injection vulnerability in links.asp in Active Price Comparison 4.0 allows remote attackers to execute arbitrary SQL commands via the linkid parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-26	7.5	CVE-2008-5975 BID FRSIRT
adnforum -- adnforum	index.php in ADN Forum 1.0b and earlier allows remote attackers to bypass authentication and gain sysop access via a fpusuario cookie composed of an initial sysop: string, an arbitrary password field, and a final :sysop:0 string.	2009-01-28	7.5	CVE-2008-6001 BID MILWORM SECUNIA
aj_square -- aj_auction	SQL injection vulnerability in sellers_othersitem.php in AJ Auction Pro Platinum 2 allows remote attackers to execute arbitrary SQL commands via the seller_id parameter.	2009-01-28	7.5	CVE-2008-6003 MILWORM
asp-project -- asp-project	Asp Project Management 1.0 allows remote attackers to bypass authentication and gain administrative access by setting the crypt cookie to 1.	2009-01-27	7.5	CVE-2009-0280 XF BID BUGTRAQ MILWORM
avbooklibrary -- avbooklibrary	Multiple SQL injection vulnerabilities in AV Book Library before 1.1 allow remote attackers to execute arbitrary SQL commands via unspecified parameters to (1) admin/edit.php, (2) admin/add.php, (3) lib/book_search.php, and possibly other components.	2009-01-29	7.5	CVE-2009-0332 XF CONFIRM CONFIRM SECUNIA
axis -- axis_camera_control	Heap-based buffer overflow in the CamImage.CamImage.1 ActiveX control in AxisCamControl.ocx in AXIS Camera Control 2.40.0.0 allows remote attackers to execute	2009-01-26	9.3	CVE-2008-5260 XF BID BUGTRAQ FRSIRT CONEDM

	arbitrary code via a long image_pan_tilt property value.			CONFIRM MISC SECUNIA OSVDB
barcodephp -- barcodegen_1d	Directory traversal vulnerability in image.php in Barcode Generator 1D (barcodegen) 2.0.0 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the code parameter.	2009-01-28	7.5	CVE-2008-5993 MILWORM
bibciter -- bibciter	Multiple SQL injection vulnerabilities in BibCiter 1.4 allow remote attackers to execute arbitrary SQL commands via the (1) idp parameter to reports/projects.php, the (2) idc parameter to reports/contacts.php, and the (3) idu parameter to reports/users.php.	2009-01-29	7.5	CVE-2009-0324 XF BID MILWORM SECUNIA CONFIRM
bmc -- patrol_agent	Format string vulnerability in BMC PATROL Agent before 3.7.30 allows remote attackers to execute arbitrary code via format string specifiers in an invalid version number to TCP port 3181, which are not properly handled when writing a log message.	2009-01-27	10.0	CVE-2008-5982 MISC SECTRACK BID BUGTRAQ FRSIRT SECUNIA
ca -- anti-spyware ca -- anti-spyware_for_the_enterprise ca -- anti-virus ca -- anti-virus_for_the_enterprise ca -- anti-virus_sdk ca -- antivirus_gateway ca -- arcserve_backup ca -- arcserve_client_agent ca -- common_services ca -- etrust_ez_antivirus ca -- etrust_intrusion_detection ca -- internet_security_suite_2007 ca -- internet_security_suite_2008 ca -- internet_security_suite_plus_2008 ca -- network_and_systems_management ca -- protection_suites ca -- secure_content_manager	Multiple unspecified vulnerabilities in the Arclib library (arclib.dll) before 7.3.0.15 in the CA Anti-Virus engine for CA Anti-Virus for the Enterprise 7.1, r8, and r8.1; Anti-Virus 2007 v8 and 2008; Internet Security Suite 2007 v3 and 2008; and other CA products allow remote attackers to bypass virus detection via a malformed archive file.	2009-01-27	10.0	CVE-2009-0042 XF BID BUGTRAQ CONFIRM

ca -- threat_manager_for_the_enterprise				
clicktech -- clickauction	SQL injection vulnerability in login_check.asp in ClickAuction allows remote attackers to execute arbitrary SQL commands via the (1) txtEmail and (2) txtPassword parameters. NOTE: some of these details are obtained from third party information.	2009-01-27	7.5	CVE-2009-0297 MILWORM SECUNIA
dark_age_cms -- dark_age_cms	SQL injection vulnerability in login.php in Dark Age CMS 0.2c beta allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-29	7.5	CVE-2009-0326 XF BID
dmxready -- blog_manager	SQL injection vulnerability in inc_webblogmanager.asp in DMXReady Blog Manager allows remote attackers to execute arbitrary SQL commands via the itemID parameter in a view action.	2009-01-29	7.5	CVE-2009-0339 XF BID BUGTRAQ SECUNIA MISC
effectmatrix -- total_video_player	Stack-based buffer overflow in EffectMatrix Total Video Player 1.31 allows user-assisted attackers to execute arbitrary code via a Skins\DefaultSkin\DefaultSkin.ini file with a large ColumnHeaderSpan value.	2009-01-23	9.3	CVE-2009-0261 XF BID MILWORM
emc -- autostart	The Backbone service (ftbackbone.exe) in EMC AutoStart before 5.3 SP2 allows remote attackers to execute arbitrary code via a packet with a crafted value that is dereferenced as a function pointer.	2009-01-27	10.0	CVE-2009-0311 MISC XF SECTRACK BID BUGTRAQ SECUNIA OSVDB
flaxweb -- flax_article_manager	SQL injection vulnerability in category.php in Flax Article Manager 1.1 allows remote attackers to	2009-01-27	7.5	CVE-2009-0284 BID

	execute arbitrary SQL commands via the cat_id parameter.	7.1		MILWORM SECUNIA
ftpshell -- ftpshell_server	Stack-based buffer overflow in FTPShell Server 4.3 allows user-assisted remote attackers to cause a denial of service (persistent daemon crash) and possibly execute arbitrary code via a long string in a licensing key (aka .key) file.	2009-01-29	9.3	CVE-2009-0349 MILWORM SECUNIA OSVDB
gdata -- antivirus_2008 gdata -- internetsecurity_2008 gdata -- totalcare_2008	The GDTdiIcpt.sys driver in G DATA AntiVirus 2008, InternetSecurity 2008, and TotalCare 2008 populates kernel registers with IOCTL 0x8317001c input values, which allows local users to cause a denial of service (system crash) or gain privileges via a crafted IOCTL request, as demonstrated by execution of the KeSetEvent function with modified register contents.	2009-01-28	7.2	CVE-2008-6000 BID FRSIRT MISC SECUNIA
gempar -- script_toko_online	SQL injection vulnerability in shop_display_products.php in Script Toko Online 5.01 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2009-01-27	7.5	CVE-2009-0296 MILWORM SECUNIA
groonesworld -- glinks	SQL injection vulnerability in index.php in Groone GLinks 2.1 allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-01-27	7.5	CVE-2009-0299 BID MILWORM SECUNIA
ipswitch -- imail	Multiple buffer overflows in Ipswitch IMail before 2006.21 allow remote attackers or authenticated users to execute arbitrary code via (1) the authentication feature in IMailsec.dll, which triggers heap corruption in the IMail Server, or (2) a long SUBSCRIBE IMAP command, which triggers a stack-based buffer overflow in the IMAP Daemon.	2009-01-27	9.0	CVE-2007-2795 CONFIRM
jadu -- jadu_cms_for_government	SQL injection vulnerability in scripts/recruit_details.php in Jadu CMS for Government allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-28	7.5	CVE-2008-5988 BID MILWORM

jetik -- jetik_emlak_sistem_a	Multiple SQL injection vulnerabilities in Jetik Emlak Sistem A (ESA) 2.0 allow remote attackers to execute arbitrary SQL commands via the KayitNo parameter to (1) diger.php and (2) sayfalar.php.	2009-01-28	7.5	CVE-2008-5992 BID MILWORM
joomla -- com_pccookbook	SQL injection vulnerability in the PcCookBook (com_pccookbook) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the recipe_id parameter in a viewrecipe action to index.php, a different vector than CVE-2008-0844.	2009-01-29	7.5	CVE-2009-0329 XF BID MILWORM
joomla -- com_waticketsystem	SQL injection vulnerability in the WebAmoeba (WA) Ticket System (com_waticketsystem) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter in a category action to index.php.	2009-01-29	7.5	CVE-2009-0333 BID SECUNIA MILWORM
katywhitton -- blogit!	SQL injection vulnerability in index.asp in Katy Whitton BlogIt! allows remote attackers to execute arbitrary SQL commands via the day parameter in an archive action.	2009-01-29	7.5	CVE-2009-0334 XF BID MILWORM SECUNIA
katywhitton -- blogit!	SQL injection vulnerability in index.asp in Katy Whitton BlogIt! allows remote attackers to execute arbitrary SQL commands via the (1) month and (2) year parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-29	7.5	CVE-2009-0337 MILWORM SECUNIA
mailwatch -- mailwatch	Directory traversal vulnerability in docs.php in MailWatch for MailScanner 1.0.4 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the doc parameter.	2009-01-28	7.5	CVE-2008-5991 BID MILWORM
	Stack-based buffer overflow in Merak Media Player 3.2 allows remote attackers to execute arbitrary			CVE-2009-0250

merak -- media_player	code via a long string in a .m3u playlist file, related to the status bar icon's tooltip. NOTE: some of these details are obtained from third party information.	2009-01-29	9.3	U3JU MILWORM SECUNIA OSVDB
microsoft -- internet_explorer	The shell32 module in Microsoft Internet Explorer 7.0 on Windows XP SP3 might allow remote attackers to execute arbitrary code via a long VALUE attribute in an INPUT element, possibly related to a stack consumption vulnerability.	2009-01-29	9.3	CVE-2009-0341 BUGTRAQ
minbank -- micronation_banking_system	Multiple PHP remote file inclusion vulnerabilities in Micronation Banking System (minba) 1.5.0 allow remote attackers to execute arbitrary PHP code via a URL in the minsoft_path parameter to (1) utdb_access.php and (2) utgn_message.php in utility/.	2009-01-30	7.5	CVE-2008-6006 XF BID MILWORM
mw6_technologies -- barcode_activex	Heap-based buffer overflow in MW6 Technologies Barcode ActiveX control (Barcode.MW6Barcode.1, Barcode.dll) 3.0.0.1 allows remote attackers to execute arbitrary code via a long Supplement property.	2009-01-27	9.3	CVE-2009-0298 BID MILWORM SECUNIA
niels_provos -- systrace	Niels Provos Systrace before 1.6f on the x86_64 Linux platform allows local users to bypass intended access restrictions by making a 64-bit syscall with a syscall number that corresponds to a policy-compliant 32-bit syscall.	2009-01-29	7.2	CVE-2009-0342 BID BUGTRAQ CONFIRM MISC MISC
niels_provos -- systrace	Niels Provos Systrace 1.6f and earlier on the x86_64 Linux platform allows local users to bypass intended access restrictions by making a 32-bit syscall with a syscall number that corresponds to a policy-compliant 64-bit syscall, related to race conditions that occur in monitoring 64-bit processes.	2009-01-29	7.2	CVE-2009-0343 BID BUGTRAQ MISC MISC MISC
ocean12_technologies --	Multiple SQL injection vulnerabilities in Ocean12 Mailing List Manager Gold allow remote	2009-01-	7.5	CVE-2008-5978 BID

mailing_list_manager	attackers to execute arbitrary SQL commands via the Email parameter to (1) default.asp and (2) s_edit.asp.	26	1.1	BID MILWORM SECUNIA
ocp2 -- omnicon_content_platform	Absolute path traversal vulnerability in admin/fileKontrola/browser.asp in Omnicom Content Platform (OCP) 2.0 allows remote attackers to list arbitrary directories via a full pathname in the root parameter.	2009-01-28	7.8	CVE-2008-5997 BID MISC
openfreeway -- freeway	Multiple SQL injection vulnerabilities in Freeway before 1.4.3.210 allow remote attackers to execute arbitrary SQL commands via unspecified vectors involving the (1) advanced search result and (2) service resource pages.	2009-01-30	7.5	CVE-2008-6013 BID CONFIRM SECUNIA
openx -- openx	Directory traversal vulnerability in fc.php in OpenX 2.6.3 allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the MAX_type parameter.	2009-01-27	7.5	CVE-2009-0291 BID MILWORM
pardalcms -- pardalcms	SQL injection vulnerability in comentar.php in Pardal CMS 0.2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-27	7.5	CVE-2009-0279 XF BID MILWORM
preprojects -- php_jobwebsite_pro	SQL injection vulnerability in siteadmin/forgot.php in PHP JOBWEBSITE PRO allows remote attackers to execute arbitrary SQL commands via the adname parameter in a Submit action.	2009-01-26	7.5	CVE-2008-5977 XF BID MISC
quidascript -- bookmarks_favourites_script	SQL injection vulnerability in view_group.php in QuidaScript BookMarks Favourites Script (APB) allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-30	7.5	CVE-2008-6007 BID MILWORM SECUNIA
quirm -- espg	Directory traversal vulnerability in gallery/comment.php in Enhanced Simple PHP Gallery (ESPG) 1.72 allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter. NOTE: the vulnerability may be in my little	2009-01-29	7.8	CVE-2009-0331 XF BID MILWORM

	homepage Comment script. If so, then this should not be treated as a vulnerability in ESPG.			MILWORM
ralinktech -- rt73	Integer overflow in Ralink Technology USB wireless adapter (RT73) 3.08 for Windows, and other wireless card drivers including rt2400, rt2500, rt2570, and rt61, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a Probe Request packet with a long SSID, possibly related to an integer signedness error.	2009-01-27	9.3	CVE-2009-0282 BUGTRAQ SECUNIA MISC
rianxosencabos_cms -- rianxosencabos_cms	SQL injection vulnerability in scripts/links.php in Rianxosencabos CMS 0.9 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-30	7.5	CVE-2008-6014 BID MILWORM
seraphimtech -- free_bible_search_php_script	SQL injection vulnerability in readable.php in Free Bible Search PHP Script 1.0 allows remote attackers to execute arbitrary SQL commands via the version parameter.	2009-01-29	7.5	CVE-2009-0327 CONFIRM BID MILWORM SECUNIA MISC
sg_real_estate_portal -- sg_real_estate_portal	SG Real Estate Portal 2.0 allows remote attackers to bypass authentication and gain administrative access by setting the Auth cookie to 1.	2009-01-30	7.5	CVE-2008-6009 BID MILWORM
sg_real_estate_portal -- sg_real_estate_portal	SQL injection vulnerability in index.php in SG Real Estate Portal 2.0 allows remote attackers to execute arbitrary SQL commands via the page_id parameter.	2009-01-30	7.5	CVE-2008-6011 BID MILWORM MILWORM
shop-inet -- shop-inet	SQL injection vulnerability in show_cat2.php in SHOP-INET 4 allows remote attackers to execute arbitrary SQL commands via the grid parameter.	2009-01-27	7.5	CVE-2009-0292 MILWORM SECUNIA
sun -- opensolaris	Unspecified vulnerability in the kernel in OpenSolaris snv_100 through snv_102 on the Sun UltraSPARC T2 and T2+ sun4v	2009-01-26	7.8	CVE-2009-0277

	platforms allows local users to cause a denial of service (panic) via unknown vectors.	20		SUNALERT
sun -- opensolaris sun -- solaris	The kernel in Sun Solaris 10 and 11 snv_101b, and OpenSolaris before snv_108, allows remote attackers to cause a denial of service (system crash) via a crafted IPv6 packet, related to an "insufficient validation security vulnerability," as demonstrated by SunOSipv6.c.	2009-01-27	7.8	CVE-2009-0304 XF BID MILWORM FRSIRT SUNALERT SECTRACK SECUNIA FULLDISC
sun -- fire_x2100_m2 sun -- fire_x2200_m2	Unspecified vulnerability in the Embedded Lights Out Manager (ELOM) on the Sun Fire X2100 M2 and X2200 M2 x86 platforms before SP/BMC firmware 3.20 allows remote attackers to obtain privileged ELOM login access or execute arbitrary Service Processor (SP) commands via unknown vectors, aka Bug ID 6633175, a different vulnerability than CVE-2007-5717.	2009-01-29	10.0	CVE-2009-0344 SUNALERT
sun -- fire_x2100_m2 sun -- fire_x2200_m2	Unspecified vulnerability in the Embedded Lights Out Manager (ELOM) on the Sun Fire X2100 M2 and X2200 M2 x86 platforms before SP/BMC firmware 3.20 allows remote attackers to obtain privileged ELOM login access or execute arbitrary Service Processor (SP) commands via unknown vectors, aka Bug ID 6648082, a different vulnerability than CVE-2007-5717.	2009-01-29	10.0	CVE-2009-0345 SUNALERT
sunbyte -- e-flower	SQL injection vulnerability in popupproduct.php in Sunbyte e-Flower allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-26	7.5	CVE-2008-5969 BID MILWORM SECUNIA
	Multiple stack-based buffer overflows in W3C Amaya Web Browser 10.0 and 11.0 allow remote attackers to execute arbitrary code via (1) a long type parameter in an			

w3 -- amaya	input tag, which is not properly handled by the EndOfXmlAttribute function; (2) an "HTML GI" in a start tag, which is not properly handled by the ProcessStartGI function; and unspecified vectors in (3) html2thot.c and (4) xml2thot.c, related to the msgBuffer variable. NOTE: these are different vectors than CVE-2008-6005.	2009-01-28	10.0	CVE-2009-0323 MISC
w3c -- amaya_web_browser	Multiple buffer overflows in the CheckUniqueName function in W3C Amaya Web Browser 10.0.1, and possibly other versions including 11.0.1, might allow remote attackers to execute arbitrary code via "duplicated" attribute value inputs.	2009-01-28	10.0	CVE-2008-6005 CONFIRM
warhound -- walking_club	SQL injection vulnerability in login.aspx in WarHound Walking Club allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-01-27	7.5	CVE-2009-0281 XF BID MILWORM
wazzum -- wazzum_dating_software	SQL injection vulnerability in profile_view.php in Wazzum Dating Software, possibly 2.0, allows remote attackers to execute arbitrary SQL commands via the userid parameter.	2009-01-27	7.5	CVE-2009-0293 BID MILWORM SECUNIA
web-cp -- web-cp	Absolute path traversal vulnerability in sendfile.php in web-cp 0.5.7, when register_globals is enabled, allows remote attackers to read arbitrary files via a full pathname in the filelocation parameter.	2009-01-28	7.1	CVE-2008-6002 CONFIRM BID MILWORM SECUNIA
wftpserver -- winftp_ftp_server	Stack-based buffer overflow in WFTPSRV.exe in WinFTP 2.3.0 allows remote authenticated users to execute arbitrary code via a long LIST argument beginning with an * (asterisk) character.	2009-01-29	9.0	CVE-2009-0351 XF BID MILWORM FRSIRT

[Back to top](#)**Medium Vulnerabilities**

Primary	Description	Published	CVSS	Source &
---------	-------------	-----------	------	----------

Vendor -- Product	Description	Published	Score	Patch Info
aj_square -- aj_auction	Cross-site scripting (XSS) vulnerability in search.php in AJ Auction Pro Platinum 2 allows remote attackers to inject arbitrary web script or HTML via the product parameter.	2009-01-28	4.3	CVE-2008-6004 MILWORM
aobosoft -- oblog	Cross-site scripting (XSS) vulnerability in err.asp in Oblog allows remote attackers to inject arbitrary web script or HTML via the message parameter.	2009-01-27	4.3	CVE-2009-0283 BID BUGTRAQ
apple -- cups	CUPS on Mandriva Linux 2008.0, 2008.1, 2009.0, Corporate Server (CS) 3.0 and 4.0, and Multi Network Firewall (MNF) 2.0 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/pdf.log temporary file.	2009-01-27	6.9	CVE-2009-0032 XF BID MANDRIVA MANDRIVA MANDRIVA SECTRACK
apple -- safari	Apple Safari 3.2.1 (aka AppVer 3.525.27.1) on Windows allows remote attackers to cause a denial of service (infinite loop or access violation) via a link to an http URI in which the authority (aka hostname) portion is either a (1) . (dot) or (2) .. (dot dot) sequence.	2009-01-28	4.3	CVE-2009-0321 BID MISC
autonomy -- ultraseek	Open redirect vulnerability in cs.html in the Autonomy (formerly Verity) Ultraseek search engine allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the url parameter.	2009-01-29	5.8	CVE-2009-0347 CERT-VN MISC MISC
bbsxp -- bbsxp	Cross-site scripting (XSS) vulnerability in error.asp in BBSXP 5.13 and earlier allows remote attackers to inject arbitrary web script or HTML via the message parameter.	2009-01-27	4.3	CVE-2009-0285 XF BID BUGTRAQ
	Cross-site scripting (XSS) vulnerability in index.php in Check Point Connectra NGX R62			

checkpoint -- connectra_nginx	HFA_01 allows remote attackers to inject arbitrary web script or HTML via the dir parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-28	4.3	CVE-2008-5994 BID SECUNIA
csound -- csound	Untrusted search path vulnerability in the (1) "VST plugin with Python scripting" and (2) "VST plugin for writing score generators in Python" in Csound 5.08.2, and possibly other versions, allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2008-5986 CONFIRM MLIST CONFIRM
dia -- dia	Untrusted search path vulnerability in the Python plugin in Dia 0.96.1, and possibly other versions, allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2008-5984 CONFIRM XF BID MLIST SECUNIA CONFIRM
dmxready -- blog_manager	Cross-site scripting (XSS) vulnerability in inc_webblogmanager.asp in DMXReady Blog Manager allows remote attackers to inject arbitrary web script or HTML via the CategoryID parameter in a refer action.	2009-01-29	4.3	CVE-2009-0338 XF BID BUGTRAQ SECUNIA MISC
drupal -- ajax_checklist	Multiple SQL injection vulnerabilities in the ajax_checklist_save function in the Ajax Checklist module 5.x before 5.x-1.1 for Drupal allow remote authenticated users, with "update ajax checklists" permissions, to execute arbitrary	2009-01-28	6.0	CVE-2008-5998 BID CONFIRM

	SQL commands via a save operation, related to the (1) nid, (2) qid, and (3) state parameters.			
eduforge -- emergecolab	Directory traversal vulnerability in connect/init.inc in emergecolab 1.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the sitecode parameter to connect/index.php.	2009-01-28	6.8	CVE-2008-5990 XF BID MILWORM
gnome -- epiphany	Untrusted search path vulnerability in the Python interface in Epiphany 2.22.3, and possibly other versions, allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2008-5985 CONFIRM MLIST CONFIRM
gnome -- eog	Untrusted search path vulnerability in the Python interface in eog 2.22.3, and possibly other versions, allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2008-5987 CONFIRM MLIST CONFIRM
gnome -- gedit	Untrusted search path vulnerability in the Python module in gedit allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2009-0314 CONFIRM MLIST MISC
	Untrusted search path vulnerability in the Python language bindings for Nautilus (nautilus-python) allows local users to execute arbitrary code	2009-01-		CVE-2009-0317

gnome -- nautilus-python	users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	US-11 CONFIRM MLIST
gnome -- gnumeric	Untrusted search path vulnerability in the GObject Python interpreter wrapper in Gnumeric allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2009-0318 CONFIRM MLIST
grid2000 -- flexcell_grid_control	Multiple insecure method vulnerabilities in the FlexCell.Grid ActiveX control (FlexCell.ocx) in FlexCell Grid Control 5.6.9 allow remote attackers to create and overwrite arbitrary files via the (1) SaveFile and (2) ExportToXML methods.	2009-01-27	6.8	CVE-2009-0301 BID MILWORM SECUNIA
hardkap -- pritlog	Directory traversal vulnerability in index.php in Pritlog 0.4 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter in a viewEntry action.	2009-01-30	4.3	CVE-2008-6012 BID
herongyang -- hybook	hyBook Guestbook Script stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing a password via a direct request for hyBook.mdb.	2009-01-30	5.0	CVE-2008-6008 XF BUGTRAQ SECUNIA
i-netsolution -- orkut_clone	SQL injection vulnerability in profile_social.php in i-Net Solution Orkut Clone allows remote authenticated users to execute arbitrary SQL commands via the id parameter.	2009-01-26	6.5	CVE-2008-5970 BID SECUNIA MISC
	Cross-site scripting (XSS) vulnerability in profile_social.php			CVE-2008-5071

i-netsolution -- orkut_clone	in i-Net Solution Orkut Clone allows remote authenticated users to inject arbitrary web script or HTML via the id parameter.	2009-01-26	4.3	S2711 BID SECUNIA MISC
isc -- bind	Internet Systems Consortium (ISC) BIND 9.6.0 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077 and CVE-2009-0025.	2009-01-26	5.0	CVE-2009-0265 CONFIRM FRSIRT SLACKWARE SECUNIA MISC
itlpoll -- itpoll	SQL injection vulnerability in index.php in Information Technology Light Poll Information (ITLPoll) 2.7 Stable 2, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-01-27	6.8	CVE-2009-0295 BID MILWORM SECUNIA
katywhitton -- blogit!	Cross-site scripting (XSS) vulnerability in index.asp in Katy Whitton BlogIt! allows remote attackers to inject arbitrary web script or HTML via the view parameter.	2009-01-29	4.3	CVE-2009-0335 XF BID MILWORM SECUNIA
katywhitton -- blogit!	Katy Whitton BlogIt! stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing user credentials via a direct request for database/Blog.mdb. NOTE: some of these details are obtained from third party information.	2009-01-29	5.0	CVE-2009-0336 XF MILWORM
kegel -- winetricks	winetricks before 20081223 allows local users to overwrite arbitrary files via a symlink attack on the x_showmenu.txt temporary file.	2009-01-27	6.9	CVE-2009-0313 BID CONFIRM
	fs/ecryptfs/inode.c in the eCryptfs			

linux -- kernel	subsystem in the Linux kernel before 2.6.28.1 allows local users to cause a denial of service (fault or memory corruption), or possibly have unspecified other impact, via a readlink call that results in an error, leading to use of a -1 return value as an array index.	2009-01-26	4.9	CVE-2009-0269 BID
linux -- kernel	drivers/firmware/dell_rbu.c in the Linux kernel before 2.6.27.13, and 2.6.28.x before 2.6.28.2, allows local users to cause a denial of service (system crash) via a read system call that specifies zero bytes from the (1) image_type or (2) packet_size file in /sys/devices/platform/dell_rbu/.	2009-01-28	4.9	CVE-2009-0322 BID
microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Microsoft Windows XP, Server 2003 and 2008, and Vista exposes I/O activity measurements of all processes, which allows local users to obtain sensitive information, as demonstrated by reading the I/O Other Bytes column in Task Manager (aka taskmgr.exe) to estimate the number of characters that a different user entered at a runas.exe password prompt, related to a "benchmarking attack."	2009-01-28	4.0	CVE-2009-0320 BID BUGTRAQ
moinmoin -- moinmoin	Multiple cross-site scripting (XSS) vulnerabilities in action/AttachFile.py in MoinMoin before 1.8.1 allow remote attackers to inject arbitrary web script or HTML via an AttachFile action to the WikiSandBox component with (1) the rename parameter or (2) the drawing parameter (aka the basename variable).	2009-01-23	4.3	CVE-2009-0260 BID
	Cross-site scripting (XSS) vulnerability in the antispam feature (security/antispam.py) in	2009-01-23	4.3	CVE-2009-0312 BID

moinmoin -- moinmoin	MoinMoin 1.7 and 1.8.1 allows remote attackers to inject arbitrary web script or HTML via crafted, disallowed content.	2009-01-27	4.3	MIL31 CONFIRM CONFIRM CONFIRM
ninjadesigns -- ninja_blog	Directory traversal vulnerability in entries/index.php in Ninja Blog 4.8, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the cat parameter.	2009-01-29	4.3	CVE-2009-0325 MISC BID MISC MILWORM SECUNIA
ocean12_technologies -- mailing_list_manager	Cross-site scripting (XSS) vulnerability in default.asp in Ocean12 Mailing List Manager Gold allows remote attackers to inject arbitrary web script or HTML via the Email parameter.	2009-01-26	4.3	CVE-2008-5979 BID MILWORM SECUNIA
ocean12_technologies -- mailing_list_manager	Ocean12 Mailing List Manager Gold stores sensitive data under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for o12mail.mdb.	2009-01-26	5.0	CVE-2008-5980 MILWORM SECUNIA
pacosdrivers -- pacpoll	PacPoll 4.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for (1) poll.mdb or (2) poll97.mdb.	2009-01-26	5.0	CVE-2008-5981 XF MILWORM
php-nuke -- downloads_module	SQL injection vulnerability in the Downloads 8.0 module for PHP-Nuke, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote authenticated users to execute arbitrary SQL commands via the url parameter in the Add operation to modules.php.	2009-01-27	4.6	CVE-2009-0302 XF BID BUGTRAQ
phpcounter -- phpcounter	Directory traversal vulnerability in defs.php in PHPcounter 1.3.2 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include	2009-01-28	6.8	CVE-2008-5989 BID MILWORM

	and execute arbitrary local files via a .. (dot dot) in the l parameter.		MILWORM SECUNIA
preprojects -- php_jobwebsite_pro	Multiple cross-site scripting (XSS) vulnerabilities in siteadmin/forgot.php in PHP JOBWEBSITE PRO allow remote attackers to inject arbitrary web script or HTML via (1) the adname parameter in a Submit action or (2) the UserName field.	2009-01-26	4.3 CVE-2008-5976 XF XF BID MISC SECUNIA
python_software_foundation -- python	Untrusted search path vulnerability in the PySys_SetArgv API function in Python before 2.6 prepends an empty string to sys.path when the argv[0] argument does not contain a path separator, which might allow local users to execute arbitrary code via a Trojan horse Python file in the current working directory.	2009-01-27	6.9 CVE-2008-5983 MLIST MLIST MLIST
quirm -- simple_php_newsletter	Multiple directory traversal vulnerabilities in Simple PHP Newsletter 1.5 allow remote attackers to read arbitrary files via a .. (dot dot) in the olang parameter to (1) mail.php and (2) mailbar.php.	2009-01-29	6.8 CVE-2009-0340 XF BID MILWORM
robs-projects -- digital_sales_ipn	ROBS-PROJECTS Digital Sales IPN (aka DS-IPN.NET or DS-IPN Paypal Shop) stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file containing user credentials via a direct request for Database/Sales.mdb.	2009-01-29	5.0 CVE-2009-0328 XF MILWORM SECUNIA
sun_netweaver	Cross-site scripting (XSS) vulnerability in Web Dynpro (WD) in the SAP NetWeaver portal, when Internet Explorer 7.0.5730 is used, allows remote	2009-01- 4.2	CVE-2008-2259

sap -- netweaver	attackers to inject arbitrary web script or HTML via a crafted URI, which causes the XSS payload to be reflected in a text/plain document.	28	4.0	2008-MISC
sg_real_estate_portal -- sg_real_estate_portal	Multiple directory traversal vulnerabilities in SG Real Estate Portal 2.0 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) mod, (2) page, or (3) lang parameter to index.php; or the (4) action or (5) folder parameter in a security request to admin/index.php.	2009-01-30	5.0	CVE-2008-6010-BID-MILWORM
sir -- gnuboard	Directory traversal vulnerability in common.php in SIR GNUBoard 4.31.03 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the g4_path parameter. NOTE: in some environments, this can be leveraged for remote code execution via a data: URI or a UNC share pathname.	2009-01-27	6.8	CVE-2009-0290-XF-BID-MILWORM-SECUNIA
sun -- opensolaris sun -- solaris	Race condition in the pseudo-terminal (aka pty) driver module in Sun Solaris 8 through 10, and OpenSolaris before snv_103, allows local users to cause a denial of service (panic) via unspecified vectors related to lack of "properly sequenced code" in ptc and ptsl.	2009-01-26	4.9	CVE-2009-0268-BID-SUNALERT-CONFIRM
sun -- java_system_application_server	Sun Java System Application Server (AS) 8.1 and 8.2 allows remote attackers to read the Web Application configuration files in the (1) WEB-INF or (2) META-INF directory via a malformed request.	2009-01-26	5.0	CVE-2009-0278-SUNALERT-CONFIRM
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the autofs module in the kernel in Sun Solaris 8 through 10, and OpenSolaris before snv_108, allows local users to cause a	2009-01-28	6.9	CVE-2009-0319-SUNALERT-EDT

sun -- solaris	denial of service (autofs mount outage) or possibly gain privileges via vectors related to "xdr processing problems."	20	SUNALERT CONFIRM
sun -- opensolaris sun -- solaris	The IP-in-IP packet processing implementation in the IPsec and IP stacks in the kernel in Sun Solaris 9 and 10, and OpenSolaris snv_01 through snv_85, allows local users to cause a denial of service (panic) via a self-encapsulated packet that lacks IPsec protection.	2009-01-29	4.9 CVE-2009-0346 SUNALERT CONFIRM
sun -- java_system_access_manager	The login module in Sun Java System Access Manager 6 2005Q1 (aka 6.3), 7 2005Q4 (aka 7.0), and 7.1 responds differently to a failed login attempt depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-01-29	5.0 CVE-2009-0348 SUNALERT CONFIRM
typo3 -- freecap_captcha_extension	Cross-site scripting (XSS) vulnerability in the freeCap CAPTCHA (sr_freecap) extension before 1.0.4 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-01-28	4.3 CVE-2008-5995 CONFIRM
vim -- vim	Untrusted search path vulnerability in the Python module in vim allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9 CVE-2009-0316 CONFIRM MLIST MLIST
webhelpdesk -- web_help_desk	Cross-site scripting (XSS) vulnerability in Web Help Desk before 9.1.18 allows remote attackers to inject arbitrary web script or HTML via vectors related to "encoded JavaScript" and Helpdesk.woa.	2009-01-27	4.3 CVE-2009-0303 BID CONFIRM SECUNIA

webmobo -- wbnews	Multiple PHP remote file inclusion vulnerabilities in WB News 2.0.1, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the config[installdir] parameter to (1) search.php, (2) archive.php, (3) comments.php, and (4) news.php; (5) News.php, (6) SendFriend.php, (7) Archive.php, and (8) Comments.php in base/; and possibly other components, different vectors than CVE-2007-1288.	2009-01-27	6.8	CVE-2009-0294 BID BUGTRAQ SECUNIA
windows_tftp_utility -- tftputil	Directory traversal vulnerability in k23productions TFTPUTil GUI 1.2.0 and 1.3.0 allows remote attackers to read arbitrary files outside the TFTP root directory via directory traversal sequences in a GET request.	2009-01-27	5.0	CVE-2009-0288 BID CONFIRM
windows_tftp_utility -- tftputil	k23productions TFTPUTil GUI 1.2.0 and 1.3.0 allows remote attackers to cause a denial of service (service crash) via a long filename in a crafted request.	2009-01-27	5.0	CVE-2009-0289 BID MISC
wss-pro -- simple_content_management_system	Directory traversal vulnerability in index.php in Simple Content Management System (SCMS) 1 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the p parameter.	2009-01-29	6.8	CVE-2009-0330 XF BID MILWORM SECUNIA
xchat -- xchat	Untrusted search path vulnerability in the Python module in xchat allows local users to execute arbitrary code via a Trojan horse Python file in the current working directory, related to a vulnerability in the PySys_SetArgv function (CVE-2008-5983).	2009-01-28	6.9	CVE-2009-0315 CONFIRM MLIST

[Back to top](#)**Low Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
drupal -- ajax_checklist	Cross-site scripting (XSS) vulnerability in the Ajax Checklist module 5.x before 5.x-1.1 for Drupal allows remote authenticated users, with create and edit permissions for posts, to inject arbitrary web script or HTML via unspecified vectors involving the ajax_checklist filter.	2009-01-28	3.5	CVE-2008-5999 CONFIRM
link3 -- simplenews	Cross-site scripting (XSS) vulnerability in the Simplenews module 5.x before 5.x-1.5 and 6.x before 6.x-1.0-beta4, a module for Drupal, allows remote authenticated users, with "administer taxonomy" permissions, to inject arbitrary web script or HTML via a Newsletter category field.	2009-01-28	3.5	CVE-2008-5996 BID CONFIRM
opengoo -- opengoo	Directory traversal vulnerability in upgrade/index.php in OpenGoo 1.1, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the form_data[script_class] parameter.	2009-01-27	2.6	CVE-2009-0286 BID MILWORM

[Back to top](#)